DEPARTMENT OF THE ARMY
HEADQUARTERS, US ARMY ARMOR CENTER AND FORT KNOX
75 6TH AVENUE
FORT KNOX, KENTUCKY 40121-5717

REPLY TO
ATTENTION OF:

Expires 15 September 2008

IMSE-KNX-IMO (25) 15 September 2006

MEMORANDUM FOR

Commanders, All Units Reporting Directly to This Headquarters
Commanders, Fort Knox Partners In Excellence
Directors and Chiefs, Staff Offices/Departments, This Headquarters

SUBJECT: Fort Knox Policy Memo No. 46-06 – Universal Serial Bus (USB) Storage Drives/Removable Devices/Media

1. References.

a. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

d. Army Activities Message 099/2006//221942Z May 06, subject: Guidance on Proper Use of Computer Hardware and Software.

2. Purpose. This memorandum outlines the procedures for USB storage drives (i.e., thumb drives, memory sticks, flash memory cards, hard drives etc.,) and removable devices/media (i.e., floppy diskettes/drives, CD-ROMs/drives, DVD ROM/drives, etc.,) used on computer equipment connected to the Fort Knox Campus Area Network (CAN).

3. Applicability. This policy applies to all Soldiers, civilians, and contractors who connect to the Fort Knox CAN.

4. Policy.

a. The USB storage drives and/removable storage devices and media must be Government purchased, government property, and be for Government use. Personal USB drives and media are not authorized for use on government equipment.

b. The USB drive must be formatted to New Technology File System (NTFS) format rather than File Allocation Table (FAT) format.

c. It is strongly recommended the USB drive be password protected in case of loss or theft.

d. The Government purchased USB drive will not be connected to privately-owned equipment.

e. The USB drive must be marked and protected according to the level of classification and sensitivity of the data stored on that media. Sensitive, mission-critical, and classified information requires protection from disclosure, alteration, and loss. While security requirements for information processed and stored electronically are no different from hard-copy (paper) requirements, information systems and storage media create a unique environment resulting in unique protection measures. Classified information protection measures are outlined in AR 380-5.

(1) Unclassified Drives: The USB storage drive must be marked with the SF 710 unclassified label. If the device is too small for the label, cut the label to fit the device.

(2) Classified Drives:

(a) If the USB storage drive is used on a classified system, it must be marked with the appropriate security classification label, secured appropriately, and included in the accreditation of the machine. It cannot be downgraded to a lower classification and will not be used on any other equipment other than for what it is classified. Classified systems and media will be labeled with the highest classification processed. SF 707 (SECRET) will be used if the classification is SECRET. If the device is too small for the label, cut the label to fit the device. Additionally, SF 712 (SCI) will be used on Sensitive Compartmented Information systems.

(b) If information is downloaded to a USB storage drive, courier orders are required if the information is to leave the secure area and in a locked container to transport the classified drive.

(c) If the drive is not hand carried, it must be transported by a designated person in the Defense Courier Service and properly wrapped, stamped, and enclosed in a GSA-approved pouch or container if leaving a secure area and going off-site.

(d) If a device containing classified information is lost or stolen, the user's IASO and commander/director must be notified immediately. The commander can assign an investigator to implement an AR 15-6 investigation to assess the damage and determine necessary procedures to mitigate the risk.

f. Devices cannot be purged or released outside DOD control. At the end-of-life cycle, the device must be destroyed.

5. Personnel are reminded that violations of these policies may be punishable under the Uniform Code of Military Justice and/or United States Code per reference d above.

FOR THE COMMANDER:

MARK D. NEEDHAM
COL, AR
Garrison Commander

DISTRIBUTION:
A